UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,013	08/17/2001	Robert J. Lambert	06944.0037-01	2945

7590 10/01/2004

Finnegan, Henderson, Farabow,
Garrett & Dunner, L.L.P.
1300 I Street, N.W.
Washington, DC 20005-3315

EXAMINER	
CHAI, LONGBIT	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/01/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/931,103	FAURE ET AL.
	Examiner	Art Unit
	Longbit Chai	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____

DETAILED ACTION

Priority

1. The application is filed on 08/17/2001 but claims the benefit of foreign priority has been made and acknowledged.

2. Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 12/24/1998 on the benefit of foreign priority date.

Specification

3. The disclosure is objected to because of the following informalities:

4. On 3rd- paragraph of Summary of Invention, the phrase "points Q(x j y)" should be corrected as "Q(x, y)".

Appropriate correction is required.

5. Further corrections for any other informality throughout the entire specification are required. See 37 CFR 1.71.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim does not distinctly describe the claimed limitations.

Double Patenting

7. Claims 1 – 11 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1 – 11 of copending Application No. 09885959. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 4 and 10 are rejected under 35 U.S.C. 102(e) as being anticipated by Miyaji (Patent Number: 6263081), hereinafter referred to as Miyaji.

9. As per claim 1 and 10, Mullin teaches a method for multiplying an elliptic curve point Q(x,y) by a scalar to provide a point kQ, the method comprising the steps of: a) selecting an elliptic curve over a finite field F such that there exists an endomorphism ψ where $\psi(Q)=.\lambda.Q$ for all points Q(x,y) on the elliptic curve, and λ is an integer (Miyaji: see for example, Column 2 Line 10 – 15 and Column 4 Line 55 – 59), b) establishing a representation of said scalar k as a combination of components K_i and said integer λ (Miyaji: see for example, Figure 7 S71 – Right box and Column 2 Line 38). c) combining said representation and said point Q to form a composite representation of a multiple

corresponding to kQ (Miyaji: see for example, Column 8 Line 22 – 65 and Column 14 Line 1 – 65) and d) computing a value corresponding to said point kQ from said composite representation of kQ (Miyaji: see for example, Column 8 Line 22 – 65 and Column 14 Line 1 – 65).

10. As pr claim 4, Miyaji teaches the claimed invention as described above (see claim 1). Miyaji further teaches representation is of the form $K_i = \sum^{i=}_{i=0} K_i \lambda^i \bmod n$ where n is the number of points on the elliptic curve (Miyaji: see for example, Figure 7 S71 – Right box).

11. Claims 12 – 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Miyaji (Patent Number: 6263081), hereinafter referred to as Miyaji, and evidenced by Menezes (Handbook of Applied Cryptography, 1997), hereinafter referred to as Menezes.

12. As pr claim 12, Miyaji teaches a method of computing a coordinate of a point kP on an elliptic curve resulting from a point multiplication of an initial point P by a scalar k, said method comprising the steps of:

a) decomposing said scalar k into a pair of components K_0, k_1 for point multiplication to obtain respective points on said curve which when combined provide said point kP (Miyaji: see for example, Column 3 Line 10).

b) determining a signed representation in non-adjacent form of each of said first and second components (Miyaji: see for example, Figure 9).

c) generating a table having a plurality of signed bit combinations contained in said representations and corresponding point multiples of said combinations to provide portions of said respective points (Miyaji: see for example, Figure 9).

d) establishing for each of said representations a window having a width less then the length of each of said representations (Miyaji: see for example, Figure 9).

e) initiating a sequential examination of said representations by said windows to obtain a position for one of said windows in one of said representations contaning a respective one of said combinations in said table (Miyaji: see for example, Column 14 Line 2 – 50 and Column 14 Line 63 – 65).

f) retrieving from said table the one of said point multiples corresponding to said respective one of said signed bit combinations in said table to obtain therefrom one of said portions (Miyaji: see for example, Column 14 Line 2 – 50 and Column 14 Line 63 – 65).

g) accumulating said portion and continuing examination of said representations with a doubling of said accumulator for each bit-wise shift of said windows to obtain a representation of said coordinate of said point kP in said accumulator (Miyaji: see for example, Abstract Line 8, Column 14 Line 33 – 35 and Figure 6 S6. This is also evidenced by Menezes because the change from "squaring" to "doubling" of said accumulator is analogous to the change of algorithm from series of exponentiation to series of multiplication as taught by Menezes – i.e. A <= AxA becomes A<=A+A=2xA).

13. As pr claim 13, Miyaji as modified teaches the claimed invention as described above (see claim 12). Miyaji as modified further teaches one of said respective points is derived from said initial point P and one of said components using an endomorphism of said curve (Miyaji: see for example, Column 4 Line 55 – 59).

14. As pr claim 14, Miyaji as modified teaches the claimed invention as described above (see claim 13). Miyaji as modified further teaches one of said respective points is derived from said initial point P and one of said components using an endomorphism of said curve (Miyaji: see for example, Figure 7 S71 – Right box).

15. As pr claim 15, Miyaji as modified teaches the claimed invention as described above (see claim 12). Miyaji as modified further teaches one of said respective points is derived from said initial point P, one of said components, and a private key (Miyaji: see for example,, Column 2 Line 10 – 15 and Column 1 Line 63 – 64).

16. As pr claim 16, Miyaji as modified teaches the claimed invention as described above (see claim 15). Miyaji as modified further teaches portions of said respective points are precomputed and stored in said table (Miyaji: see for example,, Column 3 Line 37 – 39).

17. Claims 1 – 7 and 10 are rejected under 35 U.S.C. 102(e) as being anticipated by Mullin (Patent Number: 5999626), hereinafter referred to as Mullin.

18. As per claim 1 and 10, Mullin teaches a method for multiplying an elliptic curve point Q(x,y) by a scalar to provide a point kQ, the method comprising the steps of: a) selecting an elliptic curve over a finite field F such that there exists an endomorphism ψ where ψ(Q)=.λ.Q for all points Q(x,y) on the elliptic curve, and .lambda. is an integer , b) establishing a representation of said scalar k as a combination of components K_i and said integer λ. c) combining said representation and said point Q to form a composite representation of a multiple corresponding to kQ and d) computing a value corresponding to said point kQ from said composite representation of kQ (Mullin: see for example, Figure 3 & Column 5 Line 20 – 26, Column 6 Line 10 – 64).

19. As pr claim 2, Mullin teaches the claimed invention as described above (see claim 1). Mullin further teaches each of said components K_i is shorter than said scalar k (Mullin: see for example, Figure 3 & Column 5 Line 20 – 26, Column 6 Line 10 – 64).

20. As pr claim 3, Mullin teaches the claimed invention as described above (see claim 1). Mullin further teaches components K_i are initially selected and subsequently combined to provide said scalar k (Mullin: see for example, Figure 3 & Column 5 Line 20 – 26, Column 6 Line 10 – 64).

21. As pr claim 4, Mullin teaches the claimed invention as described above (see claim 1). Mullin further teaches representation is of the form $K_i = \sum^{i=}_{i=0} K_i \lambda^i \bmod n$

where n is the number of points on the elliptic curve (Mullin: see for example, Column 7 Line 62 – 64 and Column 7 Line 3 – 5).

22. As pr claim 5, Mullin teaches the claimed invention as described above (see claim 4). Mullin further teaches representation is of the form $K_0 + k_1$ (Mullin: see for example, Column 2 Line 50 – 53 and Column 7 Line 25 – 26).

23. As pr claim 6, Mullin teaches the claimed invention as described above (see claim 1). Mullin further teaches scalar k has a predetermined value and said components k (Mullin: see for example, Column 5 Line 25 – 26).

24. As pr claim 7, Mullin teaches the claimed invention as described above (see claim 3). Mullin further teaches value of said multiple kQ is calculated using simultaneous multiple addition (Mullin: see for example, Column 10 Line 4 – 6).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

25. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mullin (Patent Number: 5999626), hereinafter referred to as Mullin, in view of Menezes (Handbook of Applied Cryptography, 1997), hereinafter referred to as Menezes.

26. As per claim 8, Mullin teaches the claimed invention as described above (see claim 7). Mullin does not teach grouped terms G_I utilized in said simultaneous multiple addition are precomputed.

27. Menezes teaches grouped terms G_I utilized in said simultaneous multiple addition are precomputed (Menezes: see for example, Page 618: G_I is defined in Sec 14.88 and simultaneous multiple addition is analogous to simultaneous multiple exponentiation as taught by Menezes).

28. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Menezes within the system of Mullin because Menezes teaches an efficient method for multiplying two elements in the Group G to perform efficient exponentiation (Menezes: see for example, 2nd Paragraph of Section 14.6).

29. As per claim 9, Mullin teaches the claimed invention as described above (see claim 6). Mullin further teaches components K_i are obtained by obtaining short basis vectors (U_0, U_1) of the field F, designating a vector v as (k,O), converting v from a standard, orthonomal basis to the (U_0, U_1) basis (Mullin: see for example, Column 10 Line 35 – 39).

30. Mullin does not teach to obtain fractions f_0 f_1 representative of the vector v, applying said fractions to k to obtain a vector z, calculating an efficient equivalent v' to the vector v and using components of the vector v' in the composite representation of kQ.

31. Menezes teaches, based on normal basis and standard Euclidean algorithm, to obtain fractions f_0 f_1 representative of the vector v, applying said fractions to k to obtain a vector z, calculating an efficient equivalent v' to the vector v and using components of the vector v' in the composite representation of kQ (Menezes: see for example, Section 2.107 and Section 14.4: Extended Euclidian Algorithm and Extended g.c.d Algorithm).

32. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Menezes within the system of Mullin because Menezes teaches an efficient method for multiplying two elements in the Group G to perform efficient exponentiation (Menezes: see for example, 2nd Paragraph of Section 14.6).

33. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mullin (Patent Number: 5999626), hereinafter referred to as Mullin, in view of Reiter (Patent Number: 6243467), hereinafter referred to as Reiter.

34. As per claim 9, Mullin teaches the claimed invention as described above (see claim 6). Mullin further teaches components K_i are obtained by obtaining short basis vectors (U_0, U_1) of the field F, designating a vector v as (k,O), converting v from a standard, orthonomal basis to the (U_0, U_1) basis (Mullin: see for example, Column 10 Line 35 – 39).

35. Mullin does not teach to obtain fractions f_0 f_1 representative of the vector v, applying said fractions to k to obtain a vector z, calculating an efficient equivalent v' to

the vector v and using components of the vector v' in the composite representation of kQ.

36. Reiter also teaches components K_i are obtained by obtaining short basis vectors (U_0, U_1) of the field F, designating a vector v as (k,O), converting v from a standard, orthonomal basis to the (U_0, U_1) basis (Reiter: see for example, Column 6 Line 24 – 36).

37. Reiter further teaches, based on normal basis and extended Euclidean algorithm, to obtain fractions f_0 f_1 representative of the vector v, applying said fractions to k to obtain a vector z, calculating an efficient equivalent v' to the vector v and using components of the vector v' in the composite representation of kQ (Reiter: see for example, Column 2 Line 64).

38. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Reiter within the system of Mullin because Reiter teaches providing a method of encryption utilizing elliptic curves that facilitates the computation in an efficient and effective manner by using a reduced base expansion in non-adjacent form (NAF) (Vanstone: see for example, Column 1 Line 11).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100